

REMARKS/ARGUMENTS

This paper is submitted responsive to the office action mailed August 11, 2008. Reconsideration of the application in light of the accompanying remarks and amendments is respectfully requested.

The claims have been amended to clarify the intended scope, and these amendments do not materially alter the scope of the claims.

The term "one or more" has been replaced with "an", which is more clear. "Each" has been replaced with "the", which is more clear. New claims 19-26 cover the situation where there is more than one identification code or encryption code.

The Examiner has rejected claims 1-5-11 and 14-16 under 35 USC 103 as being unpatentable over Weiss '388 in view of Weiss '512. The Examiner reads the claimed "personal code generation means" onto the token 12 and token processor 14 of Weiss '388. The token processor 14 of Weiss '388 may be used to generate a one-time, non-predictable code from inputs received both from the token 12 and from the user, and to utilize directly and/or transmit such code to the host processor where it may be utilized for such functions as identifying the individual (authentication), verifying access to a resource or inferring an encryption key as taught in Weiss '614 (see col 2, lines 57-65). The Examiner admits that Weiss '388 does not teach one or more encryption codes that are arranged to vary with time and are synchronized with the server. However, the Examiner asserts that Weiss '512 teaches an encryption key that is a one time code that is synchronized similarly to Weiss '388.

In response, firstly, the equating of the "one time code" of Weiss '388 with the "identification code" or the "encryption code" of the present claims, which change with time, is incorrect. The one time code of Weiss '388 is generated by combining a "secret user

code" read from the token with a PIN or other coded input from the user, to produce a non-predictable one-time coded response which is transmitted to the host. A time-varying value element may also be incorporated into the secret user code to ensure that a different non-predictable code will be generated for each use. Importantly, the generation of the one time code of Weiss '388 is always dependent on the input of a user. The time-varying value element is only incorporated (if at all) at the time the user makes an input to produce the non-predictable one-time coded response (See col 3, lines 3-28).

By contrast, in the present invention, both the identification code and the encryption code are arranged to change randomly at predetermined intervals of time (see page 4, lines 19-22, for example). The "one-time" code of Weiss '388 does not change randomly at predetermined intervals of time. It only changes when a user initiates the generation of a new one-time code by the token processor. However, in the present invention, once the personal code generation means and the code server are synchronized, both continue to randomly change the identification code and the encryption code independently of and in synchronization with each other at predetermined intervals. The amendments to claim 1 are intended to clarify this difference. This is an important structural difference as it enables the code server, after synchronization, to independently determine the identification code and the encryption code of the personal code generation means at any instant of time, without any recourse to codes generated by the personal code generation means, other than the identification code which has been transmitted with the encrypted data.

Secondly, Weiss '512 teaches an encryption key that may be generated as a one time code by incorporating a clock value as an additional value to the algorithm which generates the encryption key

(col 6, lines 5-26). However, an important difference in the system of Weiss '512 is that the encryption key still has to be generated or retrieved at the transmission end by a user input (col 5, line 61 to col 6, line 4). Likewise, at the receiver end the encryption key has to be received, retrieved or generated with a user input (col 7, lines 57-62). In Weiss '512 the encryption key is not independently generated at each end because in Weiss '512 there is no code server that is synchronized with the token server at the transmission end.

In other words, even is the system of Weiss '388 is combined with the encryption key of Weiss '512, neither the encryption key of Weiss '512 nor the one time code of Weiss '388 are changing randomly at predetermined intervals of time, as in the present invention. In the present invention only the identification code of the personal code generation means together with data encrypted with the current encryption code of the personal code generation means is transmitted. The code server then matches the identification code of the personal code generation means with the corresponding identification of the code server to authenticate the user and uses the corresponding encryption code to in the code server to decrypt the transmitted data. Because the code server is synchronized with the personal code generation means, it generates both the identification code and the encryption code independently of the personal code generation means and without any user input.

It is suggested by the Examiner that encryption is incorporated into Weiss '388 by reference to Weiss '614. Weiss '388 references "inferring an encryption key" as per Weiss '614. Weiss '614 describes the process of inferring an encryption key as involving using the key or code to generate a new encryption key which is itself encrypted and then transmitted along with the encryption data to the client (col 9, lines 15-35 and Fig. 2, at step 52). Hence, Weiss '388 in teaching "inferring an encryption key" does not mean

that the client is able to independently determine the encryption code of the personal code generating device at any instant of time, as in the present invention.

An earnest and thorough effort has been made to resolve all issues in this application and place same in condition for allowance. If, upon considering this response, the Examiner is of the opinion that a telephone interview could help resolve some or all of such issues, the Examiner is invited to telephone the undersigned to discuss same.

If any additional fees are required in connection with this case, it is respectfully requested that they be charged to Deposit Account No. 02-0184.

Respectfully submitted,

By /George A. Coury/
George A. Coury
Attorney for Applicants
Reg. No. 34,309
Tel: (203) 777-6628
Fax: (203) 865-0297

Date: December 11, 2008